[illegible]

www.huawei.com

[illegible] © 2018 [illegible]

前言

• 本章主要介绍如何通过技术手段获取有效信息，并针对获取的信息分析，定位安全风险与威胁。
• 数据的收集可以从互联的网络设备中采集，也可以检查提供服务的终端系统。在安全事件发生前，通过数据的监控和分析，主动分析网络的安全风险，加固网络；在安全事件发生后，通过数据的监控和分析，迅速定位安全威胁，为攻击防御与取证提供支持。

版权所有© 2018 华为技术有限公司 第3页

目标

- 学完本课程后，您将能够：
  - 描述数据监控与分析的技术手段
  - 描述数据采集的过程
  - 使用威胁定位的技术

版权所有 © 2018 华为技术有限公司

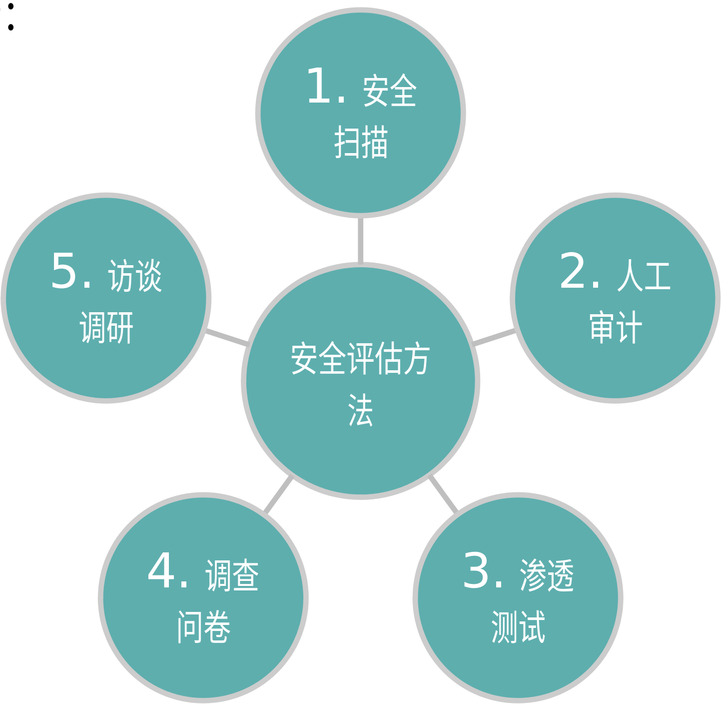
目录

1. 数据监控
   - 主动分析
   - 被动采集
2. 数据分析

版权所有 © 2018 华为技术有限公司

主动分析

- 主动分析：在攻击发生前，对网络的状况进行安全评估，对暴露的问题进行及时的改正，加固网络，提升网络的安全性。
- 安全评估方法如图所示：



版权所有 © 2018 华为技术有限公司

HUAWEI

安全扫描

安全扫描 → 人工审计 → 渗透测试 → 问卷调查 → 访谈调研

- 工作目标：为了充分了解目标系统当前的网络安全漏洞状况，需要利用扫描分析评估工具对目标系统进行扫描，以便发现相关漏洞。
- 工作内容：
  - 系统开放的端口号
  - 系统中存在的安全漏洞
  - 是否存在弱口令
  - SQL 注入漏洞
  - 跨站脚本漏洞
- 工作输出
  - 扫描工具生成结果

扫描工具

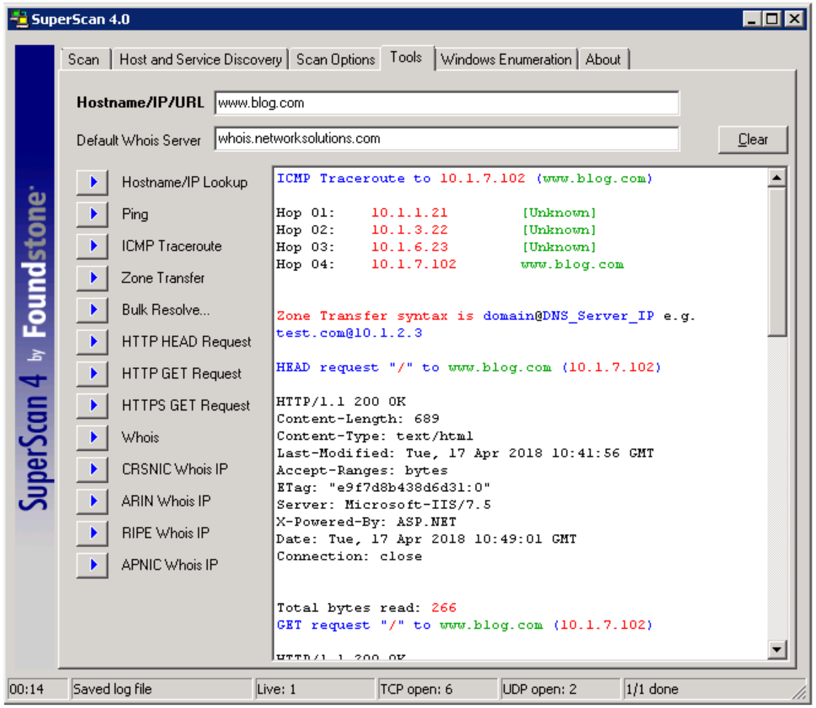
工具类型		工具名称	用途
扫描类型	端口扫描软件	superscan	功能强大的端口扫描软件： • 通过 Ping 来检验 IP 是否在线； • 检验目标计算机提供的服务类别； • 检验一定范围目标计算机的是否在线和端口情况。
		Nmap	是 Linux 下的网络扫描和嗅探工具包。基本功能：一是探测一组主机是否在线；其次是扫描 主机端口，嗅探所提供的网络服务；还可以推断主机所用的操作系统。
	漏洞扫描工具	Sparta	集成于 Kali 内的漏洞扫描工具，能够发现系统中开启的服务以及开放端口，还可以根据字典，暴力破解应用的用户名和密码。
	应用扫描	Burp Suite	Burp Suite 是用于渗透 web 应用程序的集成平台。它包含了许多工具，并为这些工具设计了许多接口，以促进加快攻击应用程序的过程。

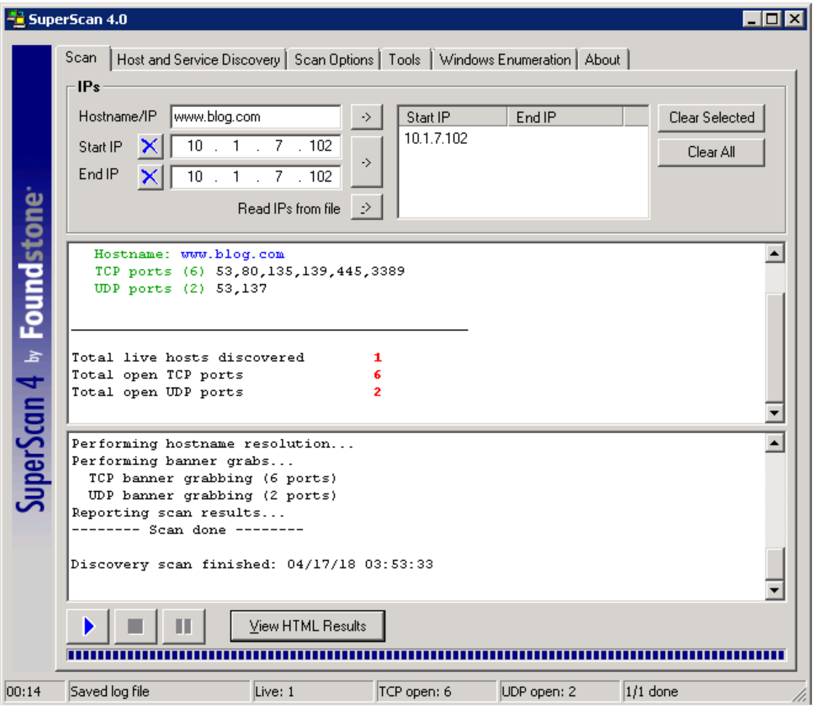
版权所有 © 2018 华为技术有限公司

Superscan 工具使用展示

• 如图，使用Superscan 对实验环境中的web服务器进行扫描，测试如图：

版权所有© 2018 华为技术有限公司 第 10页





查看 Superscan 扫描结果

- 在“ Scan” 菜单栏，点解“ View HTML Result” 查看扫描结果，如下图：

SuperScan Report - 04/17/18 03:53:19

IP	**10.1.7.102**
Hostname	www.blog.com
Netbios Name	[redacted]
Workgroup/Domain	WORKGROUP

TCP Ports (6)	
53	Domain Name Server
80	World Wide Web HTTP
135	DCE endpoint resolution
139	NETBIOS Session Service
445	Microsoft-DS
3389	MS Terminal Server

UDP Ports (2)	
53	Domain Name Server
137	NETBIOS Name Service

TCP Port	**Banner**
80 World Wide Web HTTP	HTTP/1.1 200 OK Content-Type: text/html Last-Modified: Tue, 17 Apr 2018 10:41:56 GMT Accept-Ranges: bytes ETag: "e[redacted]0" Server: Microsoft-IIS/7.5 X-Powered-By: ASP.NET Date: Tue, 17 Apr 2018 10:53:25 GMT Connection: close Content-Length: 689

UDP Port	**Banner**
137 NETBIOS Name Service	MAC Address: 0[redacted]70 NIC Vendor : Unknown Netbios Name Table (3 names) [redacted] 00 UNIQUE Workstation service name WORKGROUP 00 GROUP Workstation service name [redacted] 20 UNIQUE Server services name

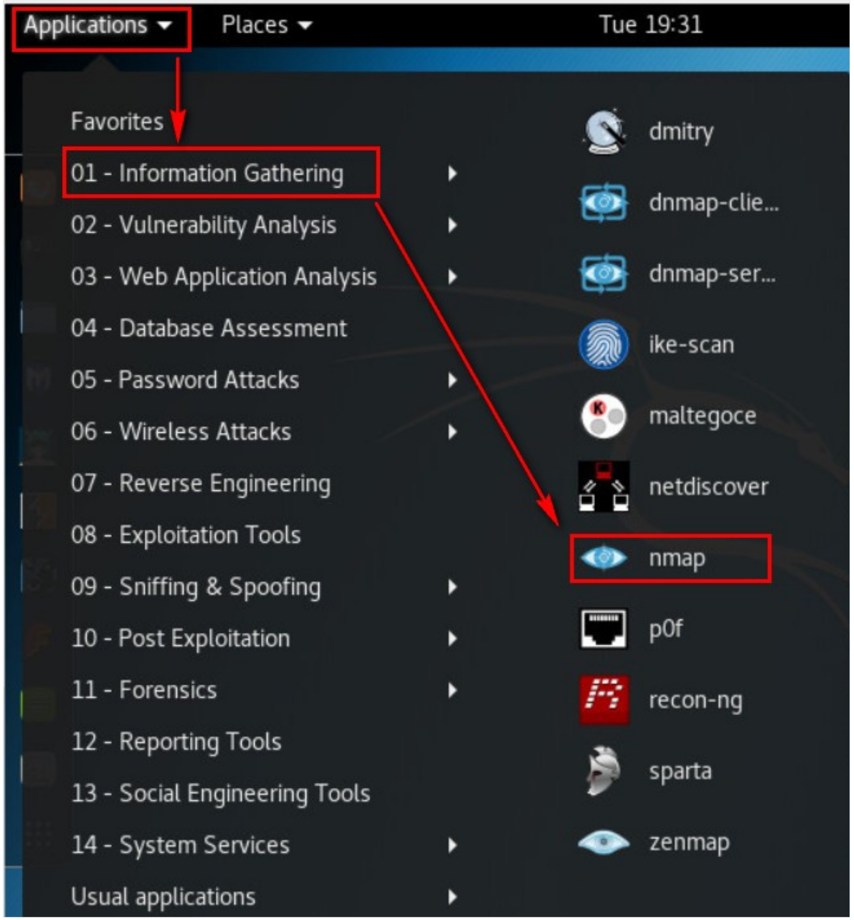
Total hosts discovered	1
Total open TCP ports	6
Total open UDP ports	2

版权所有 © 2018 华为技术有限公司

HUAWEI

Nmap 工具使用展示

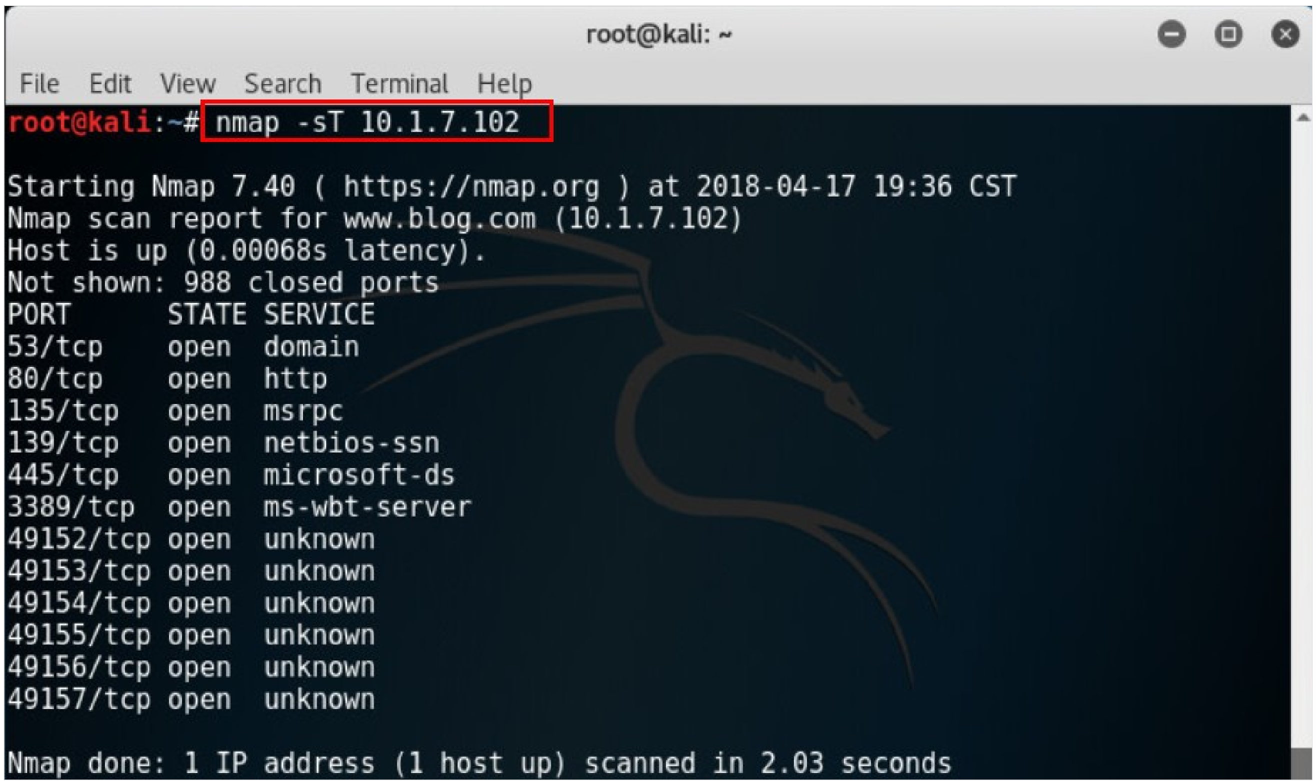
- 选择“ Application” 中的“ Information Gathering”，点击“ Nmap”，如图:



版权所有 © 2018 华为技术有限公司

查看Nmap扫描结果

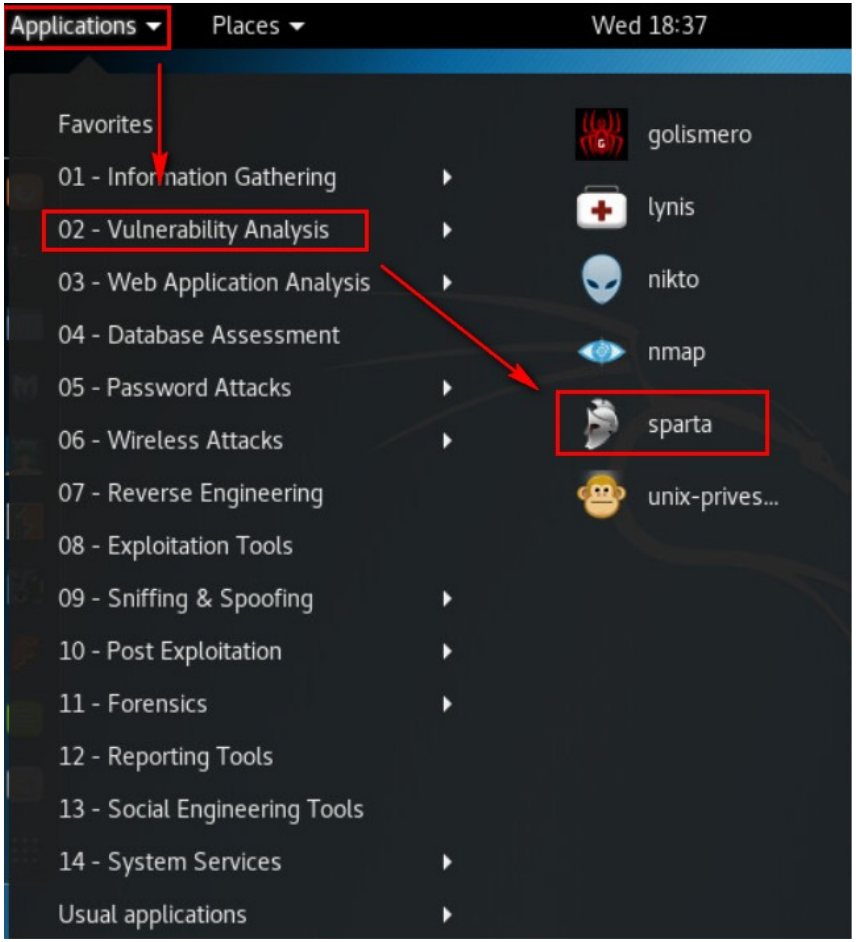
• 根据 Nmap工具的参数规则，对目标系统进行信息收集，如下图是对主机开放的TCP端口进行扫描：



版权所有© 2018 华为技术有限公司 第 13页

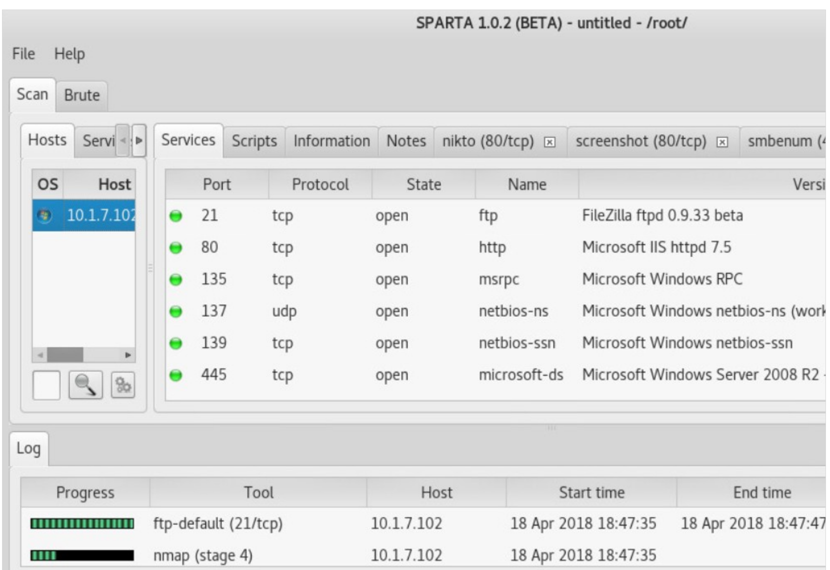
Sparta □□□□□□

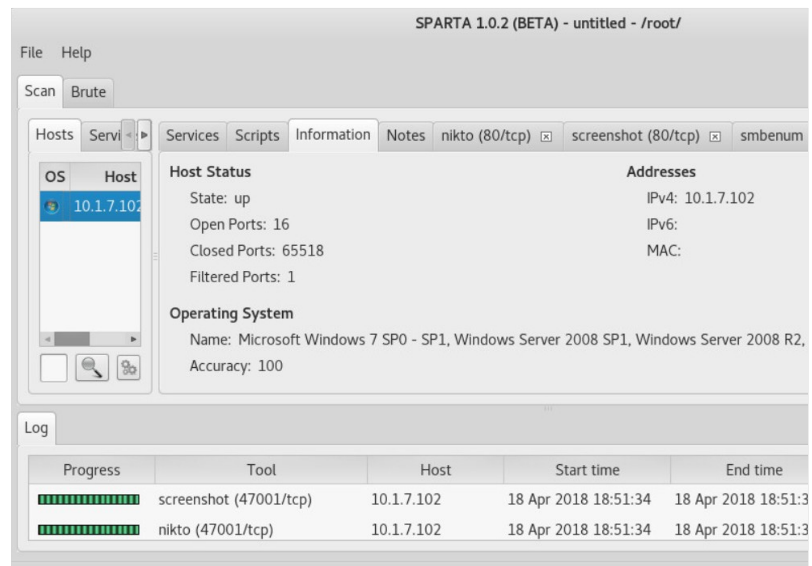
- □□“ Application” □□“ Vulnerability Analysis” □□□“ Sparta” □□□□



[illegible] Sparta [illegible]

- [illegible]

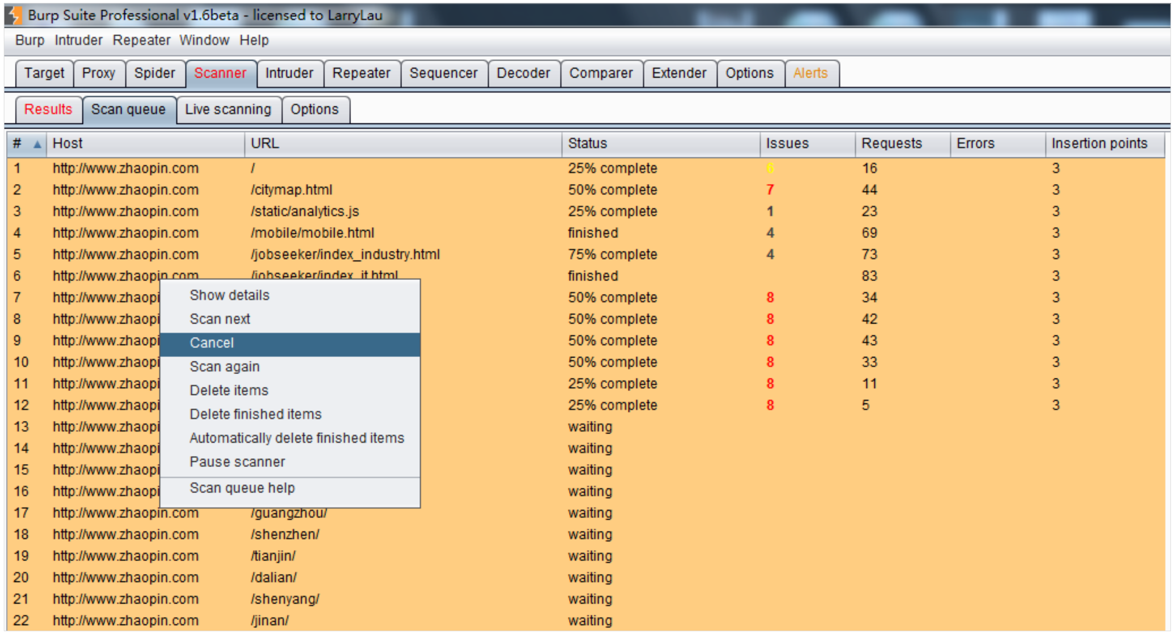

SPARTA 1.0.2 (BETA) - untitled - /root/
File Help
Scan Brute
Hosts Servi
Services Scripts Information Notes nikto (80/tcp) screenshot (80/tcp) smbenum
OS Host
10.1.7.102
Port Protocol State Name Versi
21 tcp open ftp FileZilla ftpd 0.9.33 beta
80 tcp open http Microsoft IIS httpd 7.5
135 tcp open msrpc Microsoft Windows RPC
137 udp open netbios-ns Microsoft Windows netbios-ns (work
139 tcp open netbios-ssn Microsoft Windows netbios-ssn
445 tcp open microsoft-ds Microsoft Windows Server 2008 R2
Log
Progress Tool Host Start time End time
ftp-default (21/tcp) 10.1.7.102 18 Apr 2018 18:47:35 18 Apr 2018 18:47:47
nmap (stage 4) 10.1.7.102 18 Apr 2018 18:47:35


SPARTA 1.0.2 (BETA) - untitled - /root/
File Help
Scan Brute
Hosts Servi
Services Scripts Information Notes nikto (80/tcp) screenshot (80/tcp) smbenum
OS Host
10.1.7.102
Host Status
State: up
Open Ports: 16
Closed Ports: 65518
Filtered Ports: 1
Addresses
IPv4: 10.1.7.102
IPv6:
MAC:
Operating System
Name: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2,
Accuracy: 100
Log
Progress Tool Host Start time End time
screenshot (47001/tcp) 10.1.7.102 18 Apr 2018 18:51:34 18 Apr 2018 18:51:3
nikto (47001/tcp) 10.1.7.102 18 Apr 2018 18:51:34 18 Apr 2018 18:51:3

[illegible] © 2018 [illegible]

Burp Suite 使用展示

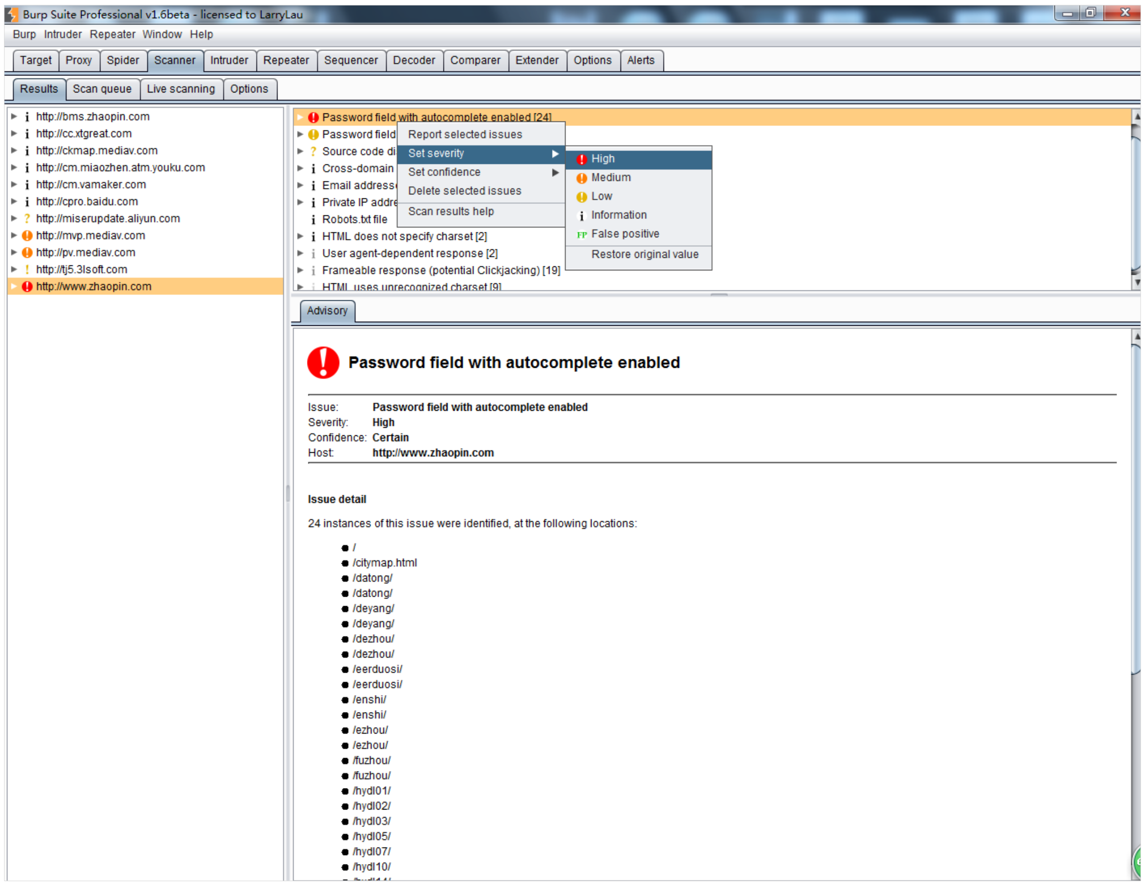
- Burp Suite 会向应用发送请求并通过 payload 验证漏洞。它对下列的两类漏洞有很好的扫描效果：
  - 客户端的漏洞，像 XSS 、Http 头注入、操作重定向；
  - 服务端的漏洞，像 SQL 注入、命令行注入、文件遍历。



版权所有 © 2018 华为技术有限公司

Burp Suite扫描结果

• 在 Results界面，自动显示队列中已经扫描完成的漏洞明细。



版权所有© 2018 华为技术有限公司 第 17页

人工审计

安全扫描 | **人工审计** | 渗透测试 | 问卷调查 | 访谈调研

- 工作目标
  - 人工审计是对工具评估的一种补充，它不需要在被评估的目标系统上安装任何软件，对目标系统的运行和状态没有任何影响，在不允许安装软件进行检查的重要主机上显得非常有用。
- 工作内容
  - 安全专家对包括主机系统、业务系统、数据库、网络设备、安全设备等在内的目标系统进行人工检查。
  - 检查的内容视检查目标不同将可能涵盖以下方面：
    - 是否安装最新补丁
    - 是否使用服务最小化原则，是否开启了不必要的服务和端口
    - 防火墙配置策略是否正确

版权所有 © 2018 华为技术有限公司

HUAWEI

渗透测试

安全扫描 → 渗透测试 → **渗透测试** → 问卷调查 → 访谈调研

- 渗透测试是作为外部审查的一部分而进行的。这种测试需要探查系统，以发现操作系统和任何网络服务，并检查这些网络服务有无漏洞。
- 渗透测试的流程如下：

1. 信息收集、分析
2. 制定渗透方案、实施准备
3. 前段信息汇报、分析
4. 提升权限、渗透实施
5. 渗透结果总结
6. 输出渗透测试报告
7. 提出安全解决建议

版权所有 © 2018 华为技术有限公司

操作运行

1. 网络管理员是否建议网络系统的配置修改记录？

A. 是　　B. 否　　C. 其他__________

2. 对网络中运行的重要服务器和路由器是否进行定期的审计和检查？

A. 是　　B. 否　　C. 其他__________

3. 对于骨干网路由器是否严格使用固定终端进行配置和管理？

A. 是　　B. 否　　C. 其他__________

4. 是否选用了网络系统运行的入侵检测设备，及时的发现和控制系统的入侵事件？

A. 是　　B. 否　　C. 其他__________

5. 在设计新应用系统时，是否考虑了将来的资源和容量需求？

A. 是　　B. 否　　C. 其他__________

6. 重要主机的管理员是都监视主要系统资源的使用情况，包括处理器、主存储器、文件存储器以及通信系统带宽？

A. 是　　B. 否　　C. 其他__________

[illegible]

[illegible] | [illegible] | [illegible] | [illegible] | **[illegible]**

- [illegible]
  - [illegible]
- [illegible]
  - [illegible]
  - [illegible]
  - [illegible]

安全管理访谈记录

序号	所属范畴	调查内容	调查结果
1	安全策略	公司是否有成体系的，统一的安全策略？	
2	安全策略	安全策略是否细化到了对信息安全各个方面的集体要求？	
3	安全策略	安全策略是否制定了专人进行维护？	
4	安全策略	是否对已公布的安全策略进行回顾，检查和发现其中不合适或已经过时的地方？	
5	安全组织	公司是否成立专门的信息安全部门或工作组负责安全管理工作？	
6	安全组织	公司是否有相关部门或领导能够协调各部门的安全管理的执行工作？	
7	安全组织	公司是否明确要求个人对个人管理的资产的安全进行负责？对于员工违背安全策略和安全流程，是否有明确的纪律处分规定？	

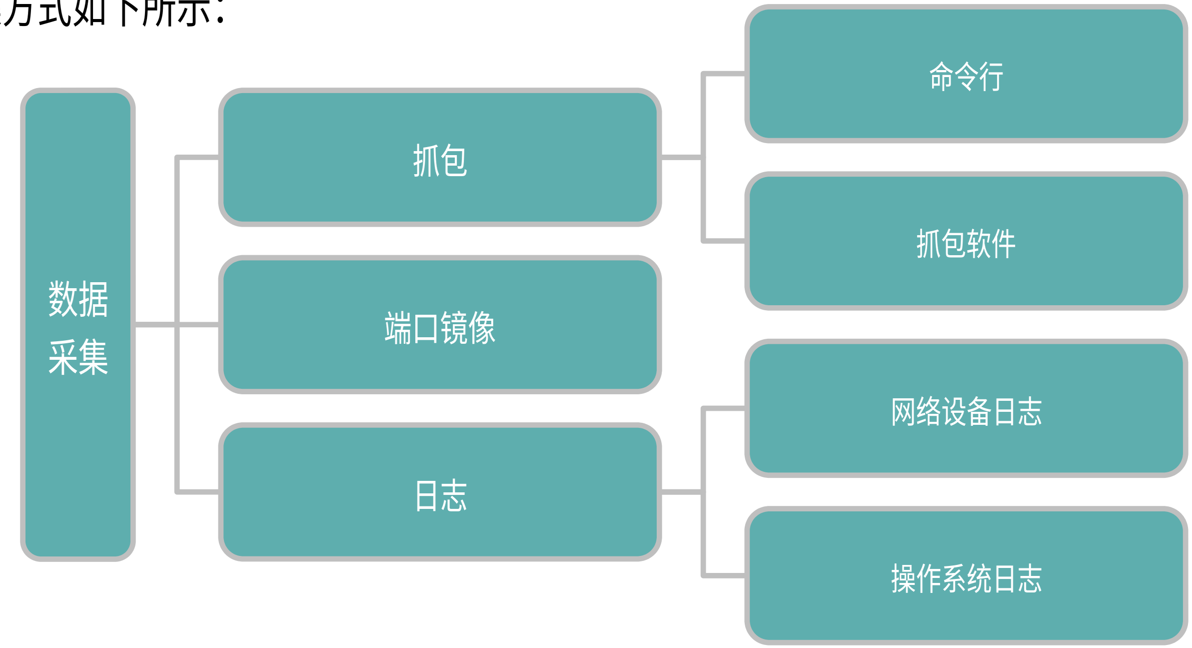
目录

1. 数据监控
   - 主动分析
   - 被动采集
2. 数据分析

版权所有 © 2018 华为技术有限公司

被动获取

- 被动获取：当攻击发生时，及时采集数据，分析攻击使用的方法，以及网络存在的问题，进行及时的补救，减少损失。
- 数据采集方式如下所示：



版权所有 © 2018 华为技术有限公司

□□ - □□□ (1)

- □□□□□□OSPF□□□□□□□

```
<Switch> debugging ospf event
Apr 12 2018 12:03:16.370.1-05:00 SW3 RM/6/RMDEBUG:
 FileID: 0x7017802d Line: 1136 Level: 0x20
  OSPF 1: Nbr 10.1.10.34 Rcv HelloReceived State Down -> Init.
Apr 12 2018 12:03:16.380.1-05:00 SW3 RM/6/RMDEBUG:
 FileID: 0x7017802d Line: 1732 Level: 0x20
  OSPF 1: Nbr 10.1.10.34 Rcv 2WayReceived State Init -> 2Way.
Apr 12 2018 12:03:16.390.1-05:00 SW3 RM/6/RMDEBUG:
 FileID: 0x7017802d Line: 1732 Level: 0x20
  OSPF 1: Nbr 10.1.10.34 Rcv AdjOk? State 2Way -> ExStart.
Apr 12 2018 12:03:16.400.1-05:00 SW3 RM/6/RMDEBUG:
 FileID: 0x7017802d Line: 1845 Level: 0x20
  OSPF 1: Nbr 10.1.10.34 Rcv NegotiationDone State ExStart -> Exchange.
Apr 12 2018 12:03:16.410.1-05:00 SW3 RM/6/RMDEBUG:
 FileID: 0x7017802d Line: 1957 Level: 0x20
  OSPF 1: Nbr 10.1.10.34 Rcv ExchangeDone State Exchange -> Loading.
Apr 12 2018 12:03:16.430.1-05:00 SW3 RM/6/RMDEBUG:
 FileID: 0x7017802d Line: 2359 Level: 0x20
  OSPF 1: Nbr 10.1.10.34 Rcv LoadingDone State Loading -> Full.
```

□□□□ © 2018 □□□□□□□□

[illegible] - [illegible] (2)

- [illegible] OSPF [illegible]

```
<Switch> debugging ospf packet
Apr 12 2018 12:05:42.930.2-05:00 SW3 RM/6/RMDEBUG:  Source Address:
10.1.10.34
Apr 12 2018 12:05:42.930.3-05:00 SW3 RM/6/RMDEBUG:  Destination Address:
224.0.0.5
Apr 12 2018 12:05:42.940.1-05:00 SW3 RM/6/RMDEBUG:  Ver# 2, Type: 1 (Hello)
Apr 12 2018 12:05:42.940.2-05:00 SW3 RM/6/RMDEBUG:  Length: 48, Router:
34.34.34.34
Apr 12 2018 12:05:42.940.3-05:00 SW3 RM/6/RMDEBUG:  Area: 0.0.0.0, Chksum:
4dcf
Apr 12 2018 12:05:42.940.4-05:00 SW3 RM/6/RMDEBUG:  AuType: 00
Apr 12 2018 12:05:42.940.5-05:00 SW3 RM/6/RMDEBUG:  Key(ascii): * * * * * * *
*d
Apr 12 2018 12:05:42.940.6-05:00 SW3 RM/6/RMDEBUG:  Net Mask: 255.255.255.0e
Apr 12 2018 12:05:42.940.7-05:00 SW3 RM/6/RMDEBUG:  Hello Int: 10, Option:
_E_
Apr 12 2018 12:05:42.940.8-05:00 SW3 RM/6/RMDEBUG:  Rtr Priority: 1, Dead
Int: 40
Apr 12 2018 12:05:42.940.9-05:00 SW3 RM/6/RMDEBUG:  DR: 10.1.10.34
Apr 12 2018 12:05:42.940.1-05:00 SW3 RM/6/RMDEBUG:  BDR: 10.1.10.33
Apr 12 2018 12:05:42.940.2-05:00 SW3 RM/6/RMDEBUG:  # Attached Neighbors: 1
Apr 12 2018 12:05:42.940.3-05:00 SW3 RM/6/RMDEBUG:  Neighbor: 33.33.33.33
```

[illegible] © 2018 [illegible]

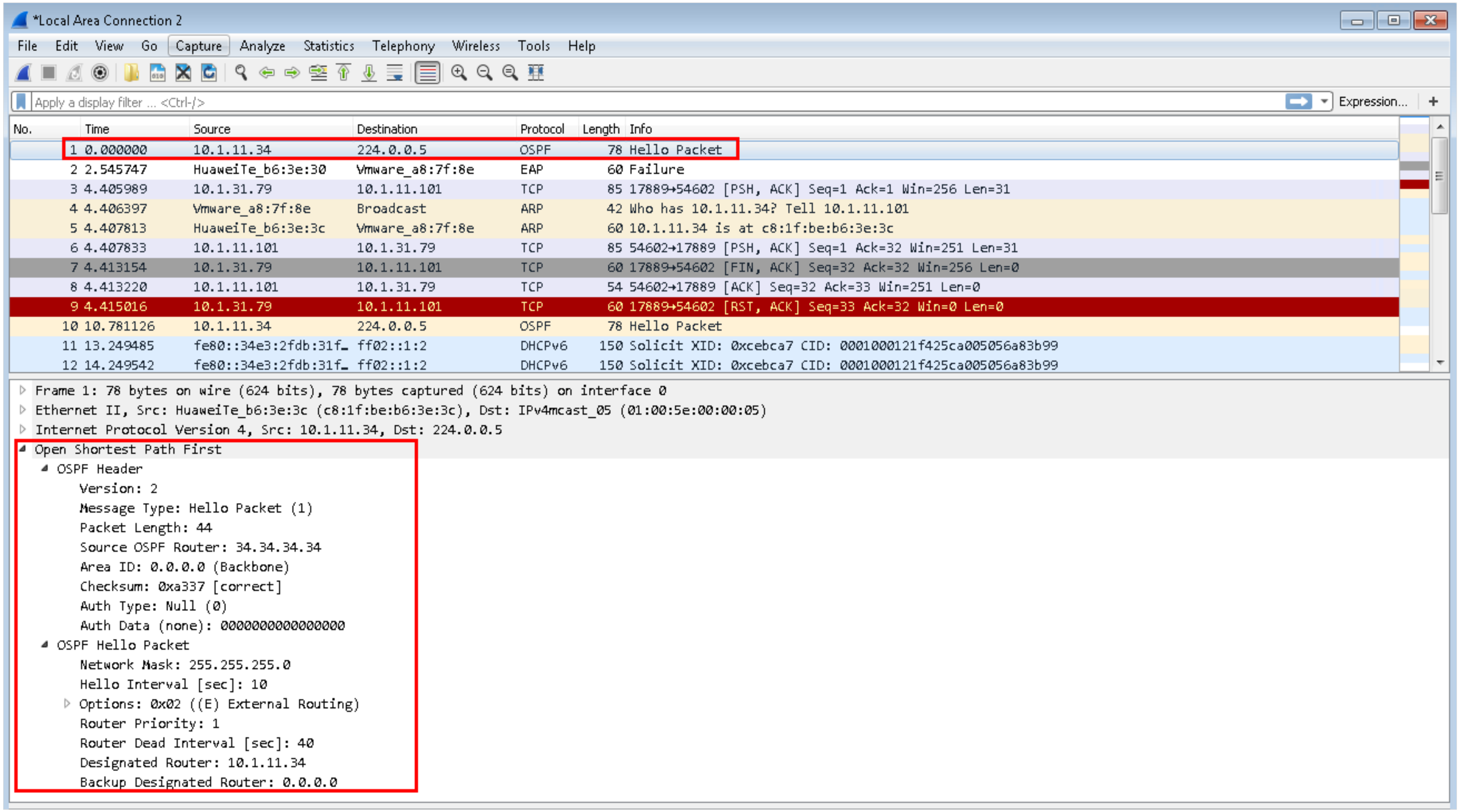
抓包 - 工具 (1)

• 使用wireshark抓包工具，查看OSPF邻居建立过程。

版权所有© 2018 华为技术有限公司 第26页

抓包 - 工具（2）

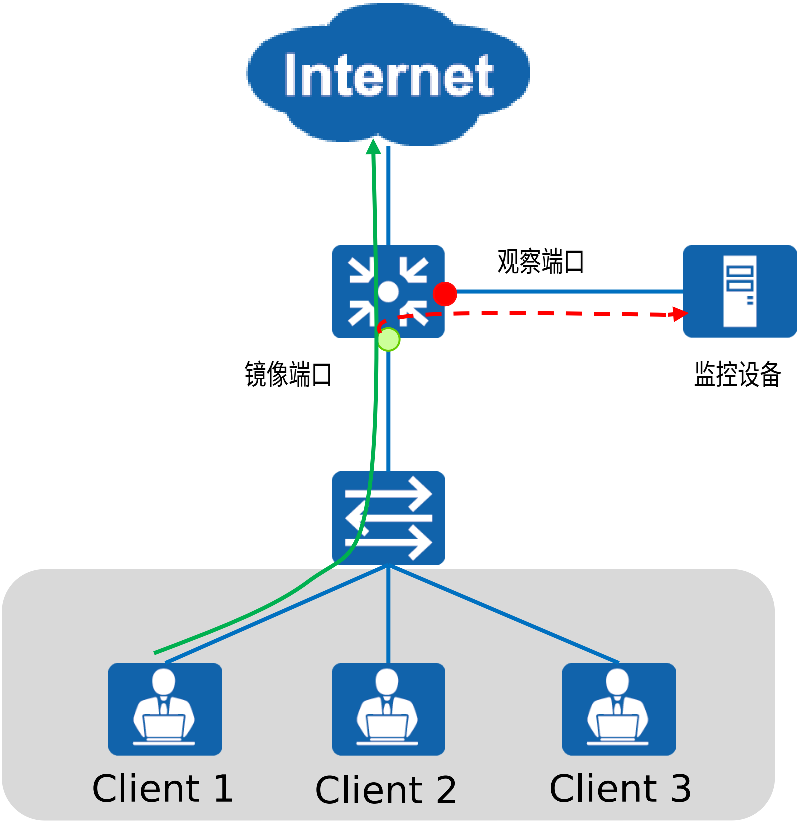
- 使用 wireshark 抓包工具，查看 OSPF 报文信息具体内容。



版权所有 © 2018 华为技术有限公司

端口镜像

- 端口镜像是指设备复制从镜像端口流经的报文，并将此报文传送到指定的观察端口进行分析和监控。



版权所有 © 2018 华为技术有限公司

HUAWEI

网络设备日志

• 以 USG6330为例，支持日志与报表，当硬盘不在位时，仅能查看并导出系统日志及业务日志。
• 硬盘不在位： • 硬盘在位：

版权所有© 2018 华为技术有限公司 第29页

防火墙日志格式

- 防火墙支持的日志格式：

格式	使用场景
二进制格式	会话日志以二进制格式输出时，占用的网络资源较少，但不能在 FW 上直接查看，需要输出到日志服务器查看。
Syslog 格式	话日志、丢包日志以及系统日志以 Syslog 格式输出时，日志的信息以文本格式呈现。
Netflow 格式	对于会话日志， FW 还支持以 Netflow 格式输出到日志服务器进行查看，便于管理员分析网络中的 IP 报文流信息。
Dataflow 格式	业务日志以 Dataflow 格式输出，在日志服务器上查看。

[illegible]

- [illegible] USG6000 [illegible]
  - [illegible]“[illegible] > [illegible] > [illegible]”[illegible]

系统日志列表

导出 刷新 请选择安全级别 查询 清除查询

安全级别	日志类型	时间	日志源	描述
警告	CFGCHECK	2018/4/13 15:49:57	FW1 %%01HRPI/4/CFGCHECK(l)[0]:	HRP checks the local and the remote devices, and the result is Different Configuration.
警告	DOWNLOAD_FAIL	2018/4/12 22:40:50	FW1 %%01UPDATE/4/DOWNLOAD_FAIL(l)[1]:	新版本下载失败。（日志序号=140，用户名=SystemTimer，IP地址=**，模块名=CNC，升级方式=auto-update，下载时长（…
警告	DOWNLOAD_FAIL	2018/4/12 22:40:43	FW1 %%01UPDATE/4/DOWNLOAD_FAIL(l)[2]:	新版本下载失败。（日志序号=139，用户名=SystemTimer，IP地址=**，模块名=IP-REPUTATION，升级方式=auto-update，…
警告	DOWNLOAD_FAIL	2018/4/12 22:40:30	FW1 %%01UPDATE/4/DOWNLOAD_FAIL(l)[3]:	新版本下载失败。（日志序号=138，用户名=SystemTimer，IP地址=**，模块名=SA-SDB，升级方式=auto-update，下载时长…
警告	DOWNLOAD_FAIL	2018/4/12 22:40:23	FW1 %%01UPDATE/4/DOWNLOAD_FAIL(l)[4]:	新版本下载失败。（日志序号=137，用户名=SystemTimer，IP地址=**，模块名=AV-SDB，升级方式=auto-update，下载时长…
警告	DOWNLOAD_FAIL	2018/4/12 22:40:10	FW1 %%01UPDATE/4/DOWNLOAD_FAIL(l)[5]:	新版本下载失败。（日志序号=136，用户名=SystemTimer，IP地址=**，模块名=IPS-SDB，升级方式=auto-update，下载时…
警告	CFGCHECK	2018/4/12 15:49:57	FW1 %%01HRPI/4/CFGCHECK(l)[6]:	HRP checks the local and the remote devices, and the result is Different Configuration.
警告	NBR_CHANGE_E	2018/4/12 11:20:01	FW1 %%01OSPF/4/NBR_CHANGE_E(l)[7]:	邻居改变事件，邻居状态改变。(进程号=1，邻居地址=10.1.50.33，邻居事件=LoadingDone，邻居先前状态=Loading，邻居…
警告	NBR_CHANGE_E	2018/4/12 11:20:01	FW1 %%01OSPF/4/NBR_CHANGE_E(l)[8]:	邻居改变事件，邻居状态改变。(进程号=1，邻居地址=10.1.50.33，邻居事件=ExchangeDone，邻居先前状态=Exchange，邻…
警告	NBR_CHANGE_E	2018/4/12 11:20:01	FW1 %%01OSPF/4/NBR_CHANGE_E(l)[9]:	邻居改变事件，邻居状态改变。(进程号=1，邻居地址=10.1.50.33，邻居事件=NegotiationDone，邻居先前状态=ExStart，…
警告	NBR_CHANGE_E	2018/4/12 11:20:01	FW1 %%01OSPF/4/NBR_CHANGE_E(l)[10]:	邻居改变事件，邻居状态改变。(进程号=1，邻居地址=10.1.50.33，邻居事件=2WayReceived，邻居先前状态=Init，邻居当…
警告	NBR_CHANGE_E	2018/4/12 11:19:54	FW1 %%01OSPF/4/NBR_CHANGE_E(l)[11]:	邻居改变事件，邻居状态改变。(进程号=1，邻居地址=10.1.50.33，邻居事件=1-Way，邻居先前状态=Full，邻居当前状态=…
错误	NBR_DOWN_REASON	2018/4/12 11:19:54	FW1 %%01OSPF/3/NBR_DOWN_REASON(l)[1…	邻居状态离开full或邻居状态Down。(进程号=1，邻居路由器标识=33.33.33.33，邻居区域ID=0，邻居接口=GigabitEtherne…

[illegible] © 2018 [illegible]

[illegible]

- [illegible] USG6000 [illegible]
  - [illegible]“[illegible] > [illegible] > [illegible]”[illegible]

业务日志列表

导出　　刷新　请选择安全级别　查询　清除查询

安全级别	日志类型	时间	日志源	描述
警告	FIREWALLATCK	2018/3/21 18:04:44	FW1 %%01ATK/4/FIREWALLATCK(l)[30]:	攻击类型="IP spoof attack", 槽位号=" ", CPU号="0", 接收接口="GE1/0/1 ", 协议=…
警告	FIREWALLATCK	2018/3/21 17:57:44	FW1 %%01ATK/4/FIREWALLATCK(l)[31]:	攻击类型="IP spoof attack", 槽位号=" ", CPU号="0", 接收接口="GE1/0/1 ", 协议=…
警告	FIREWALLATCK	2018/3/21 17:52:44	FW1 %%01ATK/4/FIREWALLATCK(l)[32]:	攻击类型="IP spoof attack", 槽位号=" ", CPU号="0", 接收接口="GE1/0/1 ", 协议=…
警告	FIREWALLATCK	2018/3/20 20:20:44	FW1 %%01ATK/4/FIREWALLATCK(l)[33]:	攻击类型="IP spoof attack", 槽位号=" ", CPU号="0", 接收接口="GE1/0/1 ", 协议=…
警告	VIRUS	2018/3/20 19:35:05	FW1 %%01AV/4/VIRUS(l)[44]:	AV检测发现病毒。(日志序号=1，虚拟系统="public"，安全策略="to_internet"，…
警告	FILTER	2018/3/18 19:19:15	FW1 %%01URL/4/FILTER(l)[45]:	命中URL过滤策略。(日志序号=1，虚拟系统="public"，安全策略="to_internet2"…
警告	BEHAVIORCTL	2018/3/18 19:04:59	FW1 %%01APPCTL/4/BEHAVIORCTL(l)[46]:	命中应用行为管控策略。(日志序号=1，虚拟系统="public"，安全策略="to_intern…
警告	DATAFILTER	2018/3/18 18:48:58	FW1 %%01DLP/4/DATAFILTER(l)[47]:	发现网络中传输包含违规字符的数据。(日志序号=3，虚拟系统="public"，安全策略…
警告	DATAFILTER	2018/3/18 18:48:11	FW1 %%01DLP/4/DATAFILTER(l)[48]:	发现网络中传输包含违规字符的数据。(日志序号=2，虚拟系统="public"，安全策略…
警告	FILEBLOCK	2018/3/18 18:18:36	FW1 %%01DLP/4/FILEBLOCK(l)[49]:	发现网络中传输违规的文件类型。(日志序号=1，虚拟系统="public"，安全策略="t…

[illegible]

- [illegible]USG6000 [illegible]
  - [illegible]“[illegible] > [illegible] > [illegible]”[illegible]

告警信息列表

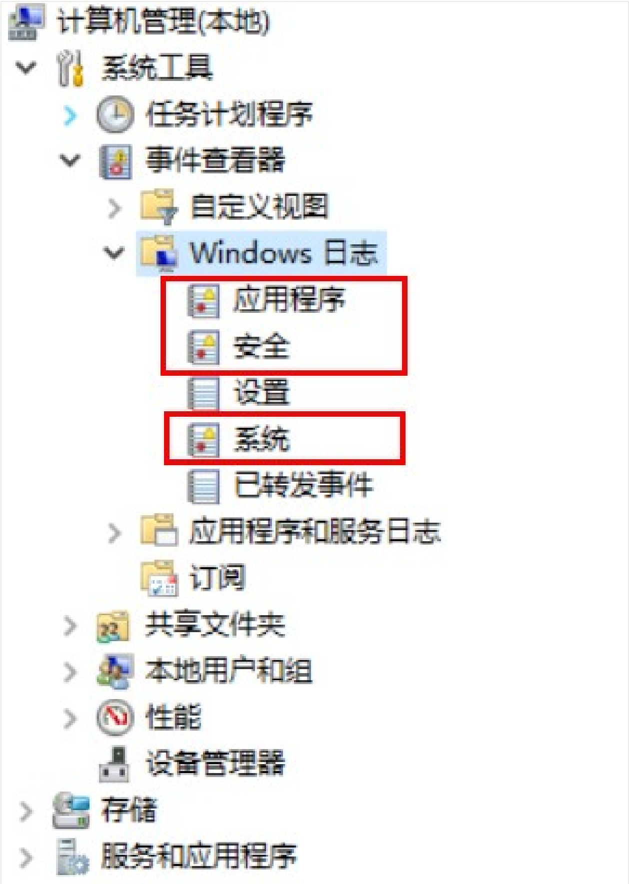
导出 刷新

级别	时间	告警源	描述
警告	2018/4/13 17:25:53	FW1 ARP/4/ARP_IPCONFLICT_TRAP:	OID 1.3.6.1.4.1.2011.5.25.123.2.6 ARP检测到IP地址冲突。（IP地址=172.21.3.150，冲突前的接口=GigabitEthernet0/0/0，冲突前的MA…
警告	2018/4/13 17:25:15	FW1 ARP/4/ARP_IPCONFLICT_TRAP:	OID 1.3.6.1.4.1.2011.5.25.123.2.6 ARP检测到IP地址冲突。（IP地址=169.254.1.1，冲突前的接口=GigabitEthernet0/0/0，冲突前的MAC…
警告	2018/4/13 17:20:28	FW1 ARP/4/ARP_IPCONFLICT_TRAP:	OID 1.3.6.1.4.1.2011.5.25.123.2.6 ARP检测到IP地址冲突。（IP地址=172.21.3.159，冲突前的接口=GigabitEthernet0/0/0，冲突前的MA…
警告	2018/4/13 17:20:19	FW1 ARP/4/ARP_IPCONFLICT_TRAP:	OID 1.3.6.1.4.1.2011.5.25.123.2.6 ARP检测到IP地址冲突。（IP地址=172.21.100.251，冲突前的接口=GigabitEthernet0/0/0，冲突前的…
警告	2018/4/13 17:18:46	FW1 ARP/4/ARP_IPCONFLICT_TRAP:	OID 1.3.6.1.4.1.2011.5.25.123.2.6 ARP检测到IP地址冲突。（IP地址=172.21.3.160，冲突前的接口=GigabitEthernet0/0/0，冲突前的MA…
警告	2018/4/13 17:15:14	FW1 ARP/4/ARP_IPCONFLICT_TRAP:	OID 1.3.6.1.4.1.2011.5.25.123.2.6 ARP检测到IP地址冲突。（IP地址=169.254.1.1，冲突前的接口=GigabitEthernet0/0/0，冲突前的MAC…
警告	2018/4/13 17:14:00	FW1 ARP/4/ARP_IPCONFLICT_TRAP:	OID 1.3.6.1.4.1.2011.5.25.123.2.6 ARP检测到IP地址冲突。（IP地址=172.21.3.163，冲突前的接口=GigabitEthernet0/0/0，冲突前的MA…
警告	2018/4/13 17:13:45	FW1 ARP/4/ARP_IPCONFLICT_TRAP:	OID 1.3.6.1.4.1.2011.5.25.123.2.6 ARP检测到IP地址冲突。（IP地址=172.21.3.161，冲突前的接口=GigabitEthernet0/0/0，冲突前的MA…
警告	2018/4/13 17:10:14	FW1 ARP/4/ARP_IPCONFLICT_TRAP:	OID 1.3.6.1.4.1.2011.5.25.123.2.6 ARP检测到IP地址冲突。（IP地址=172.21.100.251，冲突前的接口=GigabitEthernet0/0/0，冲突前的…
警告	2018/4/13 17:08:46	FW1 ARP/4/ARP_IPCONFLICT_TRAP:	OID 1.3.6.1.4.1.2011.5.25.123.2.6 ARP检测到IP地址冲突。（IP地址=172.21.3.159，冲突前的接口=GigabitEthernet0/0/0，冲突前的MA…

[illegible] © 2018 [illegible]

操作系统日志

- 以 windows 为例，点击“开始”，右键“计算机”，选择“管理”，选择“系统工具 > 事件查看器 > Windows 日志”，如下图：
- 以 windows 操作系统为例，操作系统日志分为：
  - 系统日志
  - 应用程序日志
  - 安全日志



版权所有 © 2018 华为技术有限公司

Windows 日志分类

- Windows 系统日志类型:

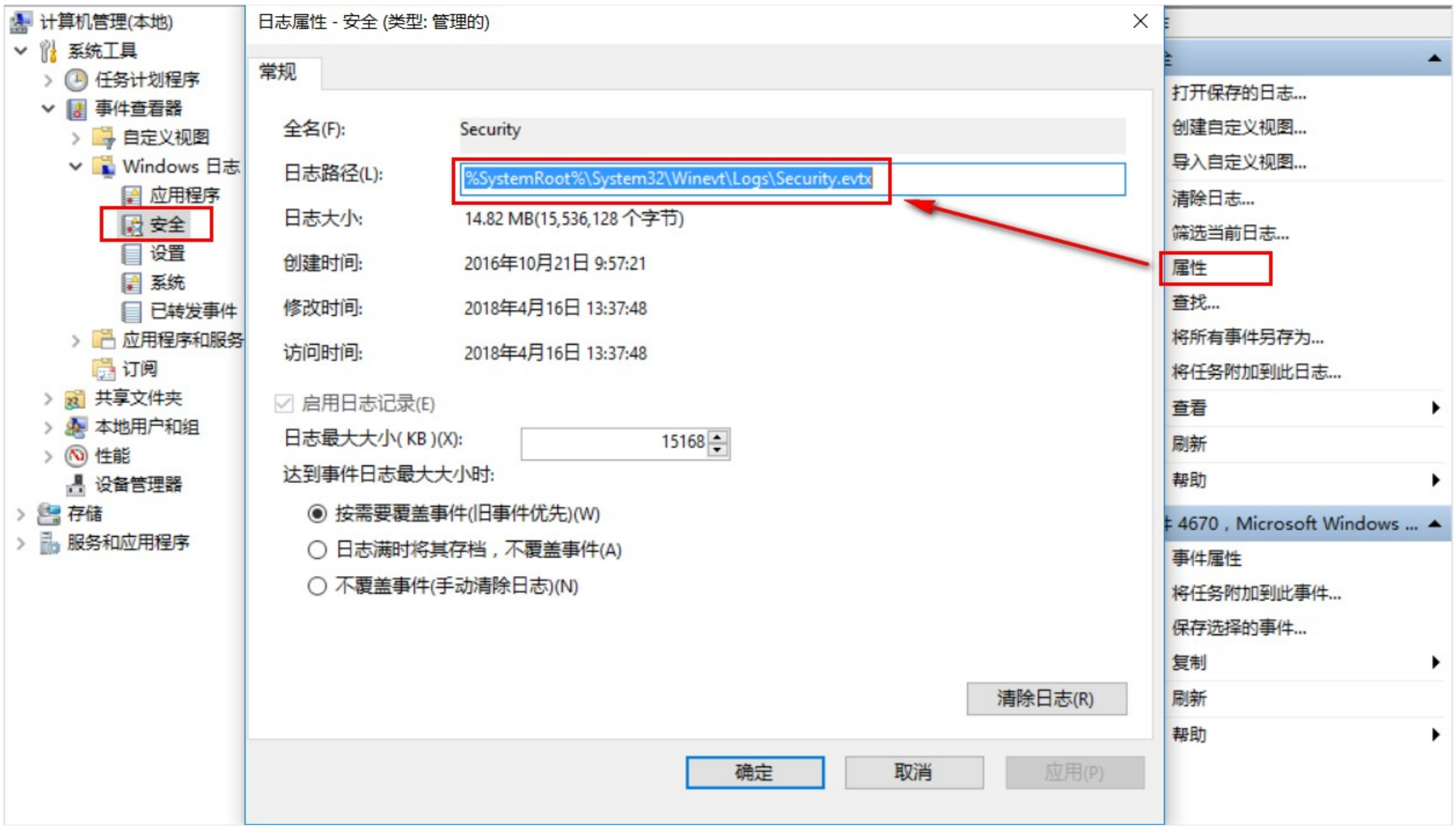
日志类型	作用	**Vista/Win7/Win8//Win10/Server 2008/Server 2012** 存储位置
系统日志	记录操作系统组件产生的事件，主要包括驱动程序、系统组件和应用软件的崩溃以及数据。	%SystemRoot%\System32\Winevt\Logs\System.evtx
应用程序日志	包含由应用程序或系统程序记录的事件，主要记录程序运行方面的事件。	%SystemRoot%\System32\Winevt\Logs\Application.evtx
安全日志	记录系统的安全审计事件，包含各种类型的登录日志、对象访问日志、进程追踪日志、特权使用、帐号管理、策略变更、系统事件。	%SystemRoot%\System32\Winevt\Logs\Security.evtx

版权所有 © 2018 华为技术有限公司

HUAWEI

Windows日志存储位置

• 以安全日志为例，选择“属性”，查看日志的具体信息，如下图：



版权所有© 2018 华为技术有限公司 第37页

Windows 日志事件类型

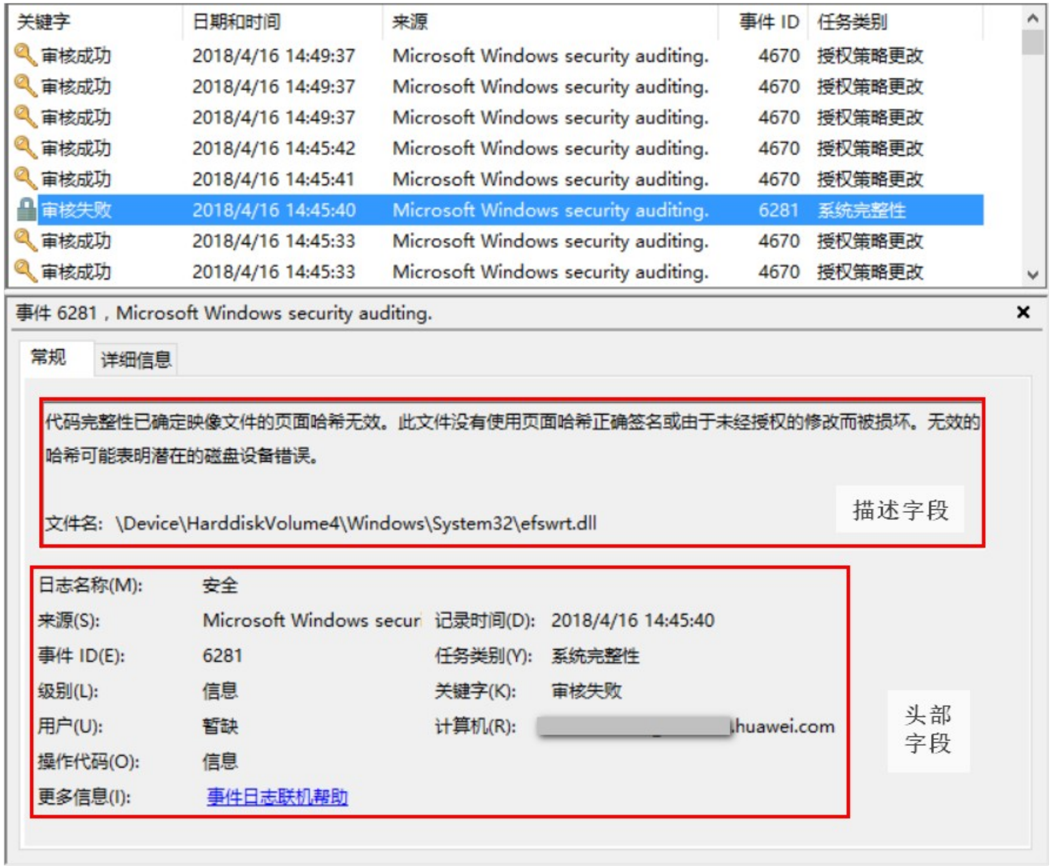
- 日志事件类型：

事件类型	作用
信息（Information）	应用程序、驱动程序或服务的成功操作的事件。
警告（Warning）	不是直接的、主要的，但是会导致将来问题的发生。例如，当磁盘空间不足或未找到打印机时，都会记录一个“警告”事件。
错误（Error）	错误事件通常指功能和数据的丢失。例如， 如果一个服务不能作为系统引导被加载，那么它会产生一个错误事件。
成功审核（Success audit）	成功的审核安全访问尝试，主要是指安全性日志，这里记录着用户登录/注销、对象访问、特权使用、账户管理、策略更改、详细跟踪、目录服务访问、账户登录等事件，例如所有的成功登录系统都会被记录为“成功审核”事件。
失败审核（Failure audit）	失败的审核安全登录尝试，例如用户试图访问网络驱动器失败，则该尝试会被作为失败审核事件记录下来。

版权所有 © 2018 华为技术有限公司

Windows 日志格式

- Windows 日志由两部分组成：头部字段和描述字段。



目录

1. 数据监控

2. 数据分析

- 日志分析
- 分析工具介绍

版权所有 © 2018 华为技术有限公司

数据分析

- 打击计算机网络犯罪的关键，是如何在计算机系统中提取和分析计算机犯罪分子留在计算机中的“痕迹”，使之成为能够追踪并抓获犯罪嫌疑人的重要手段和方法。网络中发生的重要事件都会被记录在日志中，因此，对日志的分析尤为重要。

版权所有 © 2018 华为技术有限公司

HUAWEI

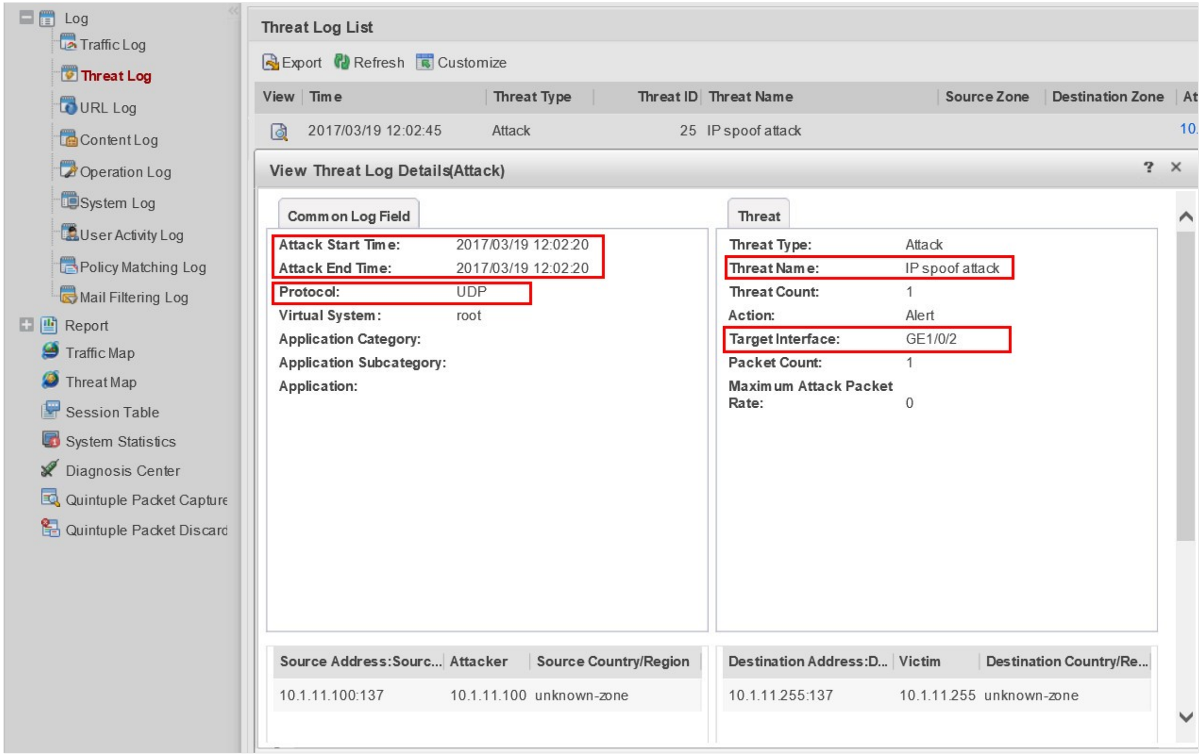
日志分析要点

- **Who**：用户、访客
- **When**：时间
- **where**：位置、设备、接口、服务
- **How**：有线、无线、VPN
- **What**：行为、设备类型、资源

版权所有 © 2018 华为技术有限公司

网络设备日志分析

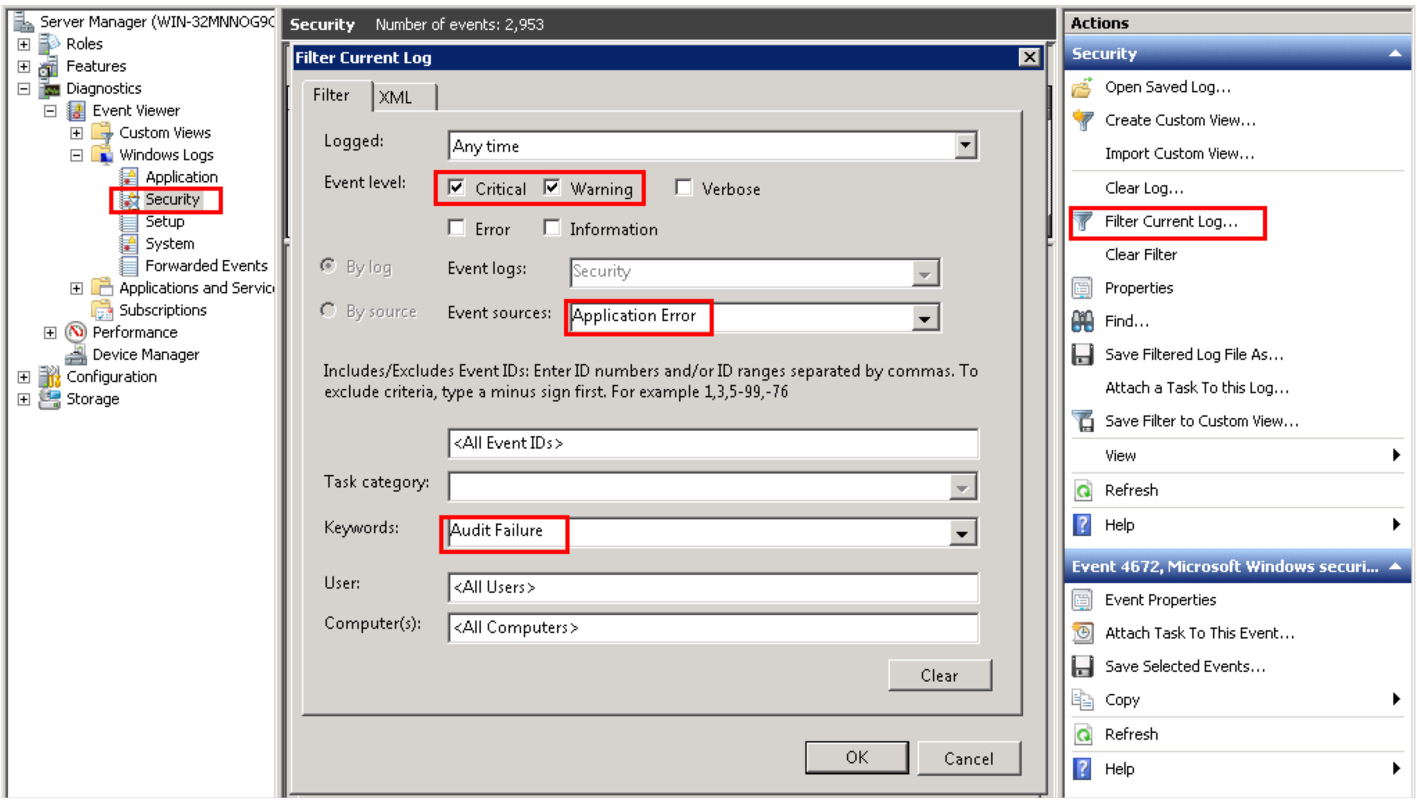
• 以防火墙为例，可以通过日志，分析攻击行为。如下图，通过“威胁日志” 发现存在 IP Spoof Attack，并可以获得攻击的时间，使用的协议，接收接口等信息。



版权所有© 2018 华为技术有限公司 第43页

[illegible]

- [illegible] Windows [illegible]
  [illegible]



Server Manager (WIN-32MNNOG9C
Roles
Features
Diagnostics
Event Viewer
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Servic
Subscriptions
Performance
Device Manager
Configuration
Storage
Security Number of events: 2,953
Filter Current Log
Filter
XML
Logged:
Any time
Event level:
Critical
Warning
Verbose
Error
Information
By log
Event logs:
Security
By source
Event sources:
Application Error
Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76
<All Event IDs>
Task category:
Keywords:
Audit Failure
User:
<All Users>
Computer(s):
<All Computers>
Clear
OK
Cancel
Actions
Security
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Clear Filter
Properties
Find...
Save Filtered Log File As...
Attach a Task To this Log...
Save Filter to Custom View...
View
Refresh
Help
Event 4672, Microsoft Windows securi...
Event Properties
Attach Task To This Event...
Save Selected Events...
Copy
Refresh
Help

用户登录与注销事件分析

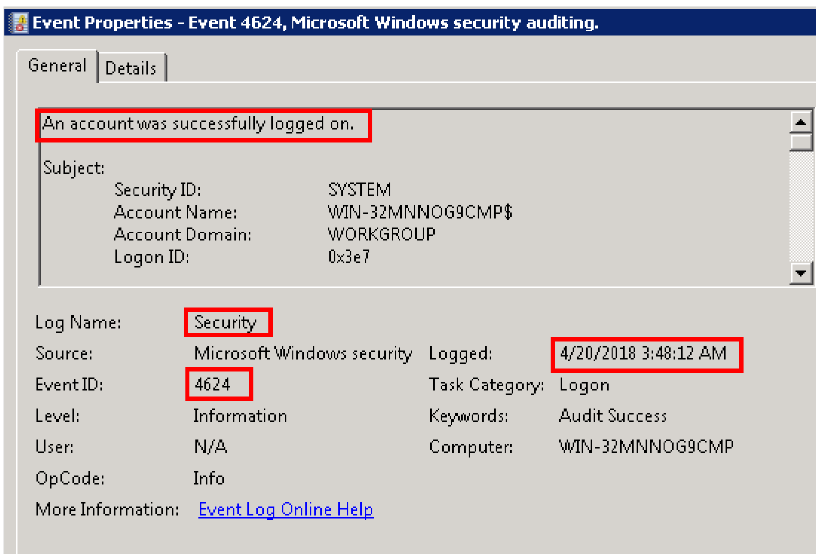
- 使用场景：
  - 判断哪些用户登录过操作系统。
  - 分析用户对操作系统的使用情况。
- 事件 ID ：
  - 4624 – 登陆成功（安全日志）
  - 4625 – 登录失败（安全日志）
  - 4634 – 注销成功（安全日志）
  - 4672 – 使用超级用户（管理员）进行登录（安全日志）

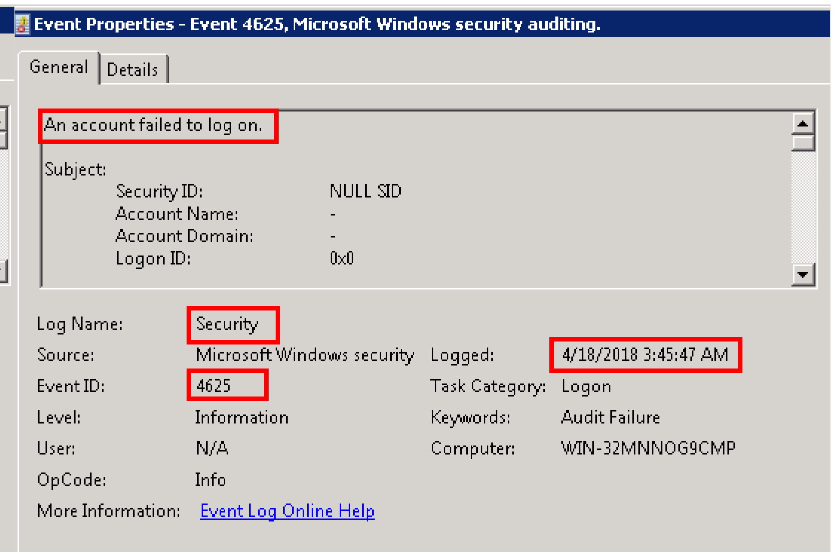
版权所有 © 2018 华为技术有限公司

HUAWEI

[illegible]

- [illegible]

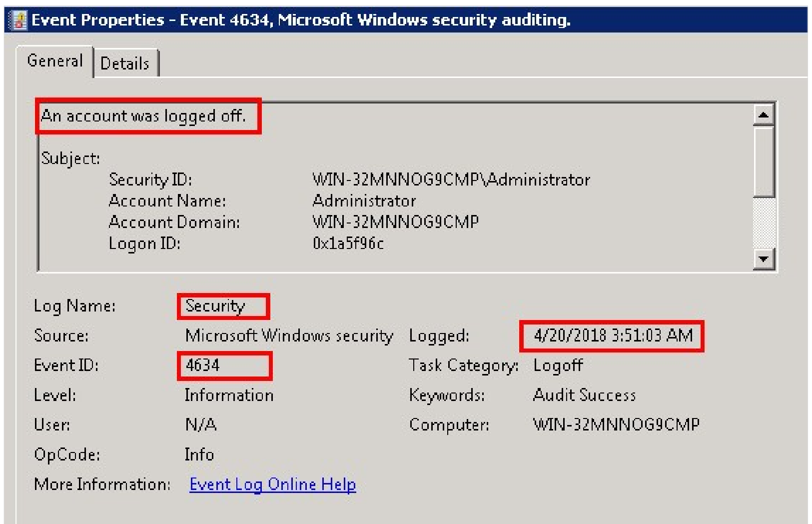

Event Properties - Event 4624, Microsoft Windows security auditing.
General
Details
An account was successfully logged on.
Subject:
Security ID: SYSTEM
Account Name: WIN-32MNNOG9CMP$
Account Domain: WORKGROUP
Logon ID: 0x3e7
Log Name: Security
Source: Microsoft Windows security
Logged: 4/20/2018 3:48:12 AM
Event ID: 4624
Task Category: Logon
Level: Information
Keywords: Audit Success
User: N/A
Computer: WIN-32MNNOG9CMP
OpCode: Info
More Information: Event Log Online Help


Event Properties - Event 4625, Microsoft Windows security auditing.
General
Details
An account failed to log on.
Subject:
Security ID: NULL SID
Account Name: -
Account Domain: -
Logon ID: 0x0
Log Name: Security
Source: Microsoft Windows security
Logged: 4/18/2018 3:45:47 AM
Event ID: 4625
Task Category: Logon
Level: Information
Keywords: Audit Failure
User: N/A
Computer: WIN-32MNNOG9CMP
OpCode: Info
More Information: Event Log Online Help

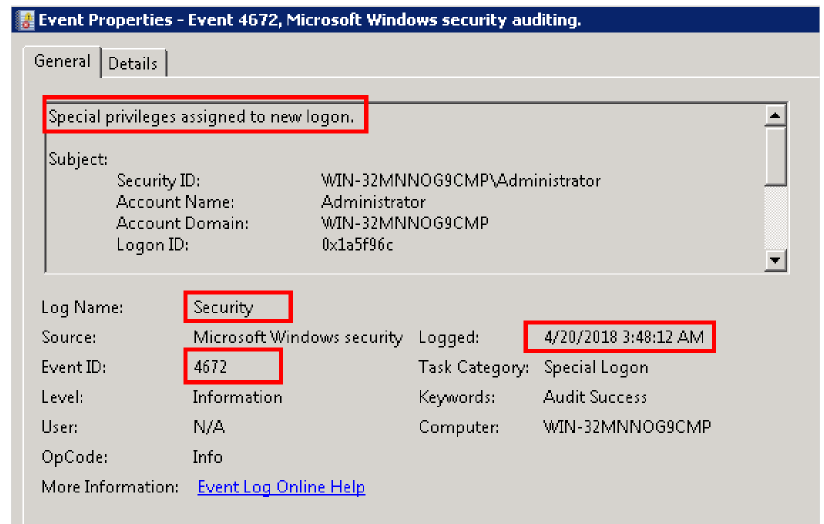
[illegible] © 2018 [illegible]

[illegible]

- [illegible]



Event Properties - Event 4634, Microsoft Windows security auditing.
General
Details
An account was logged off.
Subject:
Security ID: WIN-32MNNOG9CMP\Administrator
Account Name: Administrator
Account Domain: WIN-32MNNOG9CMP
Logon ID: 0x1a5f96c
Log Name: Security
Source: Microsoft Windows security
Logged: 4/20/2018 3:51:03 AM
Event ID: 4634
Task Category: Logoff
Level: Information
Keywords: Audit Success
User: N/A
Computer: WIN-32MNNOG9CMP
OpCode: Info
More Information: Event Log Online Help



Event Properties - Event 4672, Microsoft Windows security auditing.
General
Details
Special privileges assigned to new logon.
Subject:
Security ID: WIN-32MNNOG9CMP\Administrator
Account Name: Administrator
Account Domain: WIN-32MNNOG9CMP
Logon ID: 0x1a5f96c
Log Name: Security
Source: Microsoft Windows security
Logged: 4/20/2018 3:48:12 AM
Event ID: 4672
Task Category: Special Logon
Level: Information
Keywords: Audit Success
User: N/A
Computer: WIN-32MNNOG9CMP
OpCode: Info
More Information: Event Log Online Help

[illegible] © 2018 [illegible]

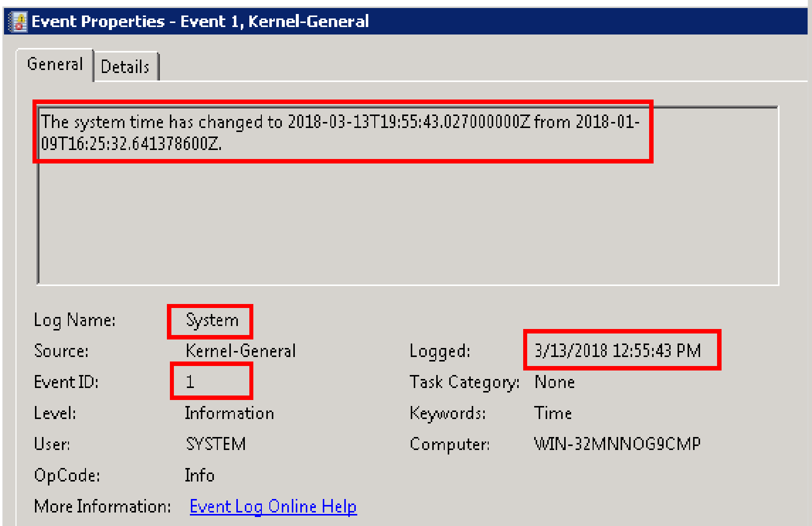
修改系统时间事件分析

- 使用场景：
  - 查找用户修改系统时间的证据。
- 事件 ID：
  - 1 – Kernel-General （系统日志）
  - 4616 – 更改系统时间（安全日志）

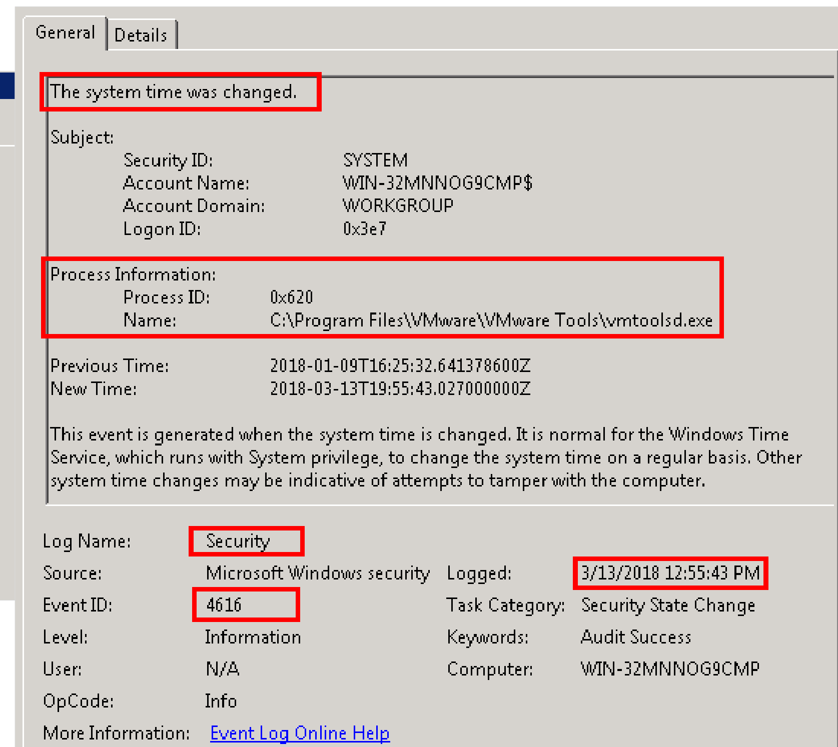
版权所有 © 2018 华为技术有限公司

[illegible]

- [illegible]



Event Properties - Event 1, Kernel-General
General
Details
The system time has changed to 2018-03-13T19:55:43.027000000Z from 2018-01-09T16:25:32.641378600Z.
Log Name: System
Source: Kernel-General
Logged: 3/13/2018 12:55:43 PM
Event ID: 1
Task Category: None
Level: Information
Keywords: Time
User: SYSTEM
Computer: WIN-32MNNOG9CMP
OpCode: Info
More Information: Event Log Online Help



General
Details
The system time was changed.
Subject:
Security ID: SYSTEM
Account Name: WIN-32MNNOG9CMP$
Account Domain: WORKGROUP
Logon ID: 0x3e7
Process Information:
Process ID: 0x620
Name: C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
Previous Time: 2018-01-09T16:25:32.641378600Z
New Time: 2018-03-13T19:55:43.027000000Z
This event is generated when the system time is changed. It is normal for the Windows Time Service, which runs with System privilege, to change the system time on a regular basis. Other system time changes may be indicative of attempts to tamper with the computer.
Log Name: Security
Source: Microsoft Windows security
Logged: 3/13/2018 12:55:43 PM
Event ID: 4616
Task Category: Security State Change
Level: Information
Keywords: Audit Success
User: N/A
Computer: WIN-32MNNOG9CMP
OpCode: Info
More Information: Event Log Online Help

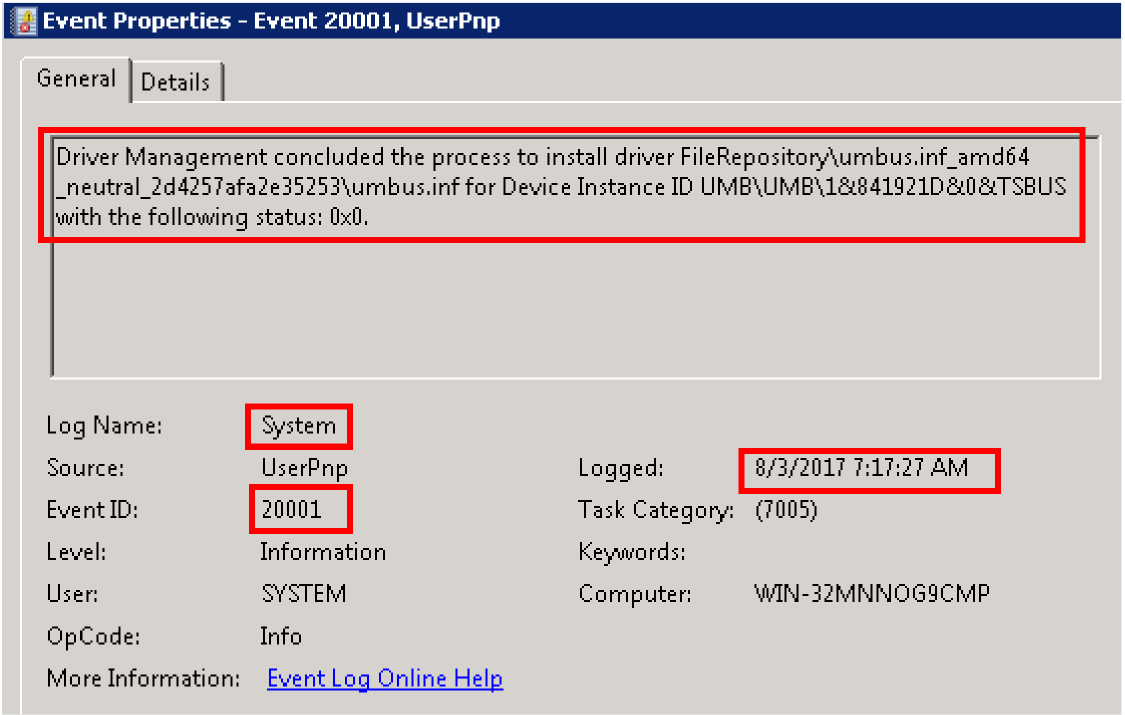
[illegible] © 2018 [illegible]

外部设置使用事件分析

- 使用场景：
  - 分析哪些硬件设备何时安装到系统中。
- 事件 ID ：
  - 20001/20003 – 即插即用驱动安装（系统日志）

[illegible]

- [illegible]


Event Properties - Event 20001, UserPnp
General
Details
Driver Management concluded the process to install driver FileRepository\umbus.inf_amd64_neutral_2d4257afa2e35253\umbus.inf for Device Instance ID UMB\UMB\1&841921D&0&TSBUS with the following status: 0x0.
Log Name: System
Source: UserPnp
Logged: 8/3/2017 7:17:27 AM
Event ID: 20001
Task Category: (7005)
Level: Information
Keywords:
User: SYSTEM
Computer: WIN-32MNNOG9CMP
OpCode: Info
More Information: Event Log Online Help

目录

1. 数据监控
2. 数据分析
   - 日志分析
   - 分析工具介绍

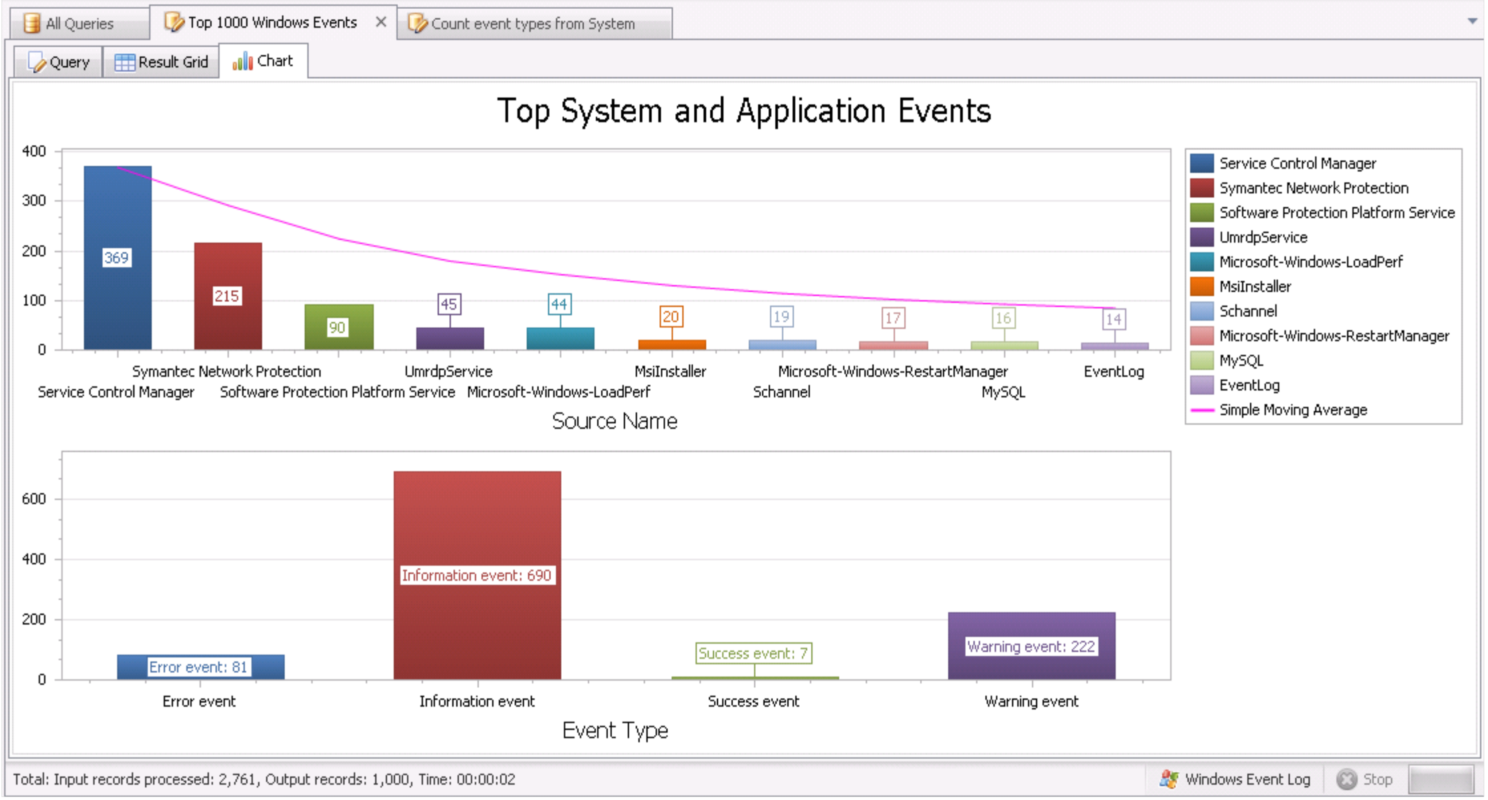
日志分析工具

• Log Parser是微软公司出品的日志分析工具，它功能强大，使用简单，可以分析基于文本的日志文件、XML 文件、CSV（逗号分隔符）文件，以及操作系统的事件日志、注册表、文件系统、Active Directory。但需要能够熟练的使用SQL语言。
• Log Parser Lizard 使用图形界面，比较易于使用，甚至不需要记忆繁琐的命令，只需要做好设置，写好基本的SQL语句，就可以直观的得到结果。

版权所有© 2018 华为技术有限公司 第53页

Log Parser Lizard 使用展示（1）

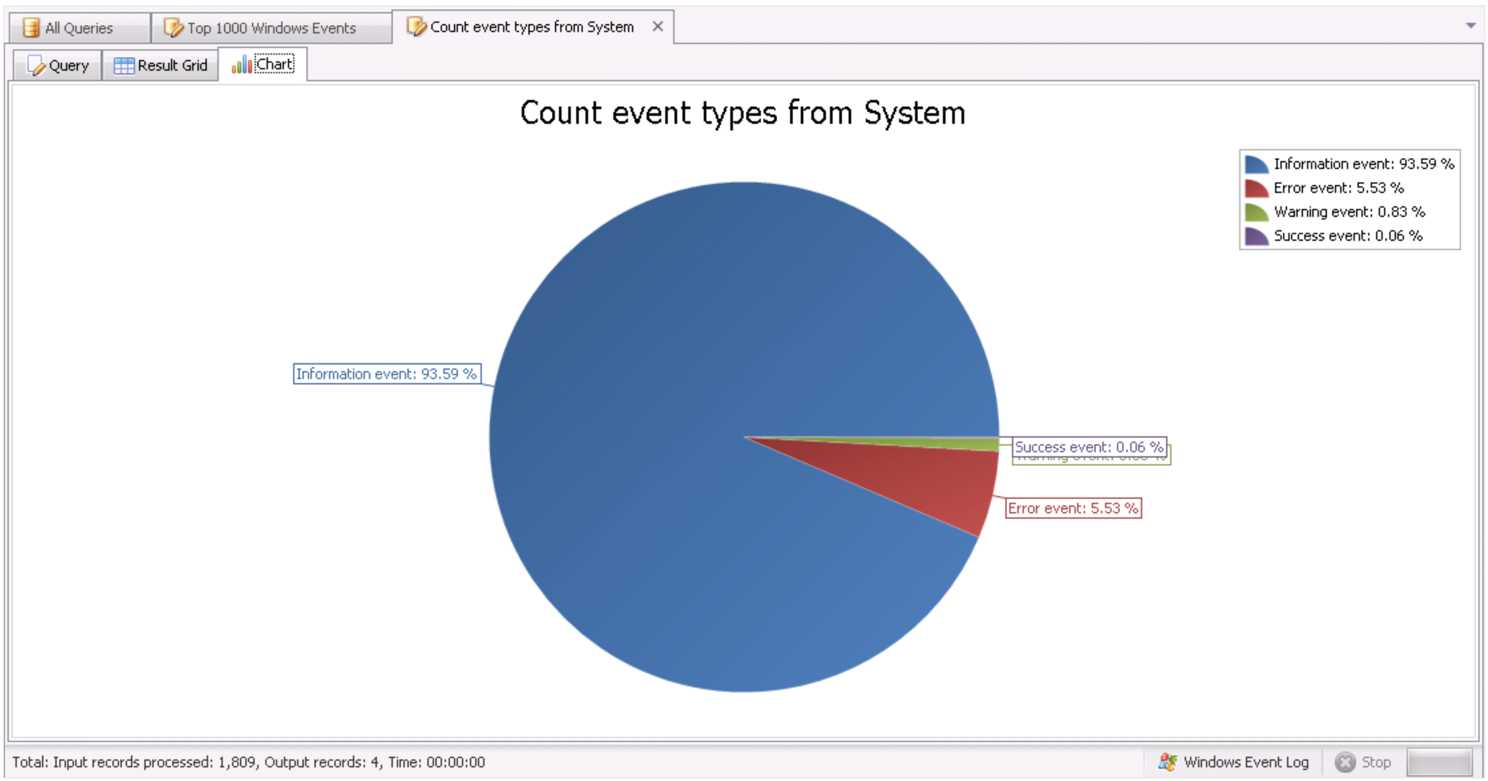
- 如图，展示了使用 Log Parser Lizard 筛选“ TOP 1000 Windows Event” 的结果。



版权所有 © 2018 华为技术有限公司

Log Parser Lizard □□□□（2)

- □□□□□□□□ Log Parser Lizard □□“ Count event types from System” □□□□



思考题

1. 安全评估方法不包括以下哪个选项？（）
   - A. 安全扫描
   - B. 人工审计
   - C. 渗透测试
   - D. 调查取证
2. Windows 日志分类不包括以下哪个选项？（）
   - A. 系统日志
   - B. 安全日志
   - C. 应用程序日志
   - D. 业务日志

版权所有 © 2018 华为技术有限公司

本章总结

- 数据监控
  - 主动分析
  - 被动采集
- 数据分析
  - 日志分析
  - 分析工具介绍

版权所有 © 2018 华为技术有限公司

www.huawei.com